REMARKS

In the Office Action, the Examiner issued a final rejection of Claims 1-18, which are all of the pending claims, as being unpatentable under 35 U.S.C. 103 over the prior art. Specifically, Claims 1-5 and 7-18 were rejected as being unpatentable over International Application WO 01/595545 (Subramaniam), U.S. Patent 5,870,473 (Boesch, et al.) and International Application WO 00/01108 (McLaughlin). Also, Claim 6 was rejected as being unpatentable over Subramanian, Boesch, et al. and U.S. Patent 5,794,207 (Walker, et al.).

Applicants herein ask that independent Claims 1, 13 and 17 be amended to better define the subject matters of these claims.

For the reasons set forth below, Claims 1-18 patentably distinguish over the prior art and are allowable. The Examiner is, accordingly, requested to enter this Amendment, to reconsider and to withdraw the above-identified rejections of Claims 1-18, and to allow these claims.

This invention provides a method and system for parties to communicate in a dialogue over a computer network. With many existing computer network dialogues, such as "chat rooms," there is no assurance that what is said is accurate or reliable. As a result, these dialogues are not suitable for many types of conversations such as business negotiations.

The present invention, in contrast to these prior art approaches, provides accountability for what is said during the dialogue. To elaborate, in accordance with the preferred embodiment of the invention, a plurality of users registers with a trusted body. To do this, each user generates a public/private key pair for a specific dialogue session and sends the public key of that pair to the trusted body. That trusted body verifies the identity of each user by using the public key sent to the trusted body. Once the identity of a user is verified,

the trusted body generates a random identifier for the user and keeps a confidential record of the relation between the identity of each user and the random identifier for that user.

One of the users enters into a dialogue with one or more other users by sending messages over the computer network and through the trusted body to said one or more other users. Each user is able to remain anonymous through use of its random identifier until such time as the user reveals it's identify to one or more of the other users. Also, the trusted body records the dialogue by encrypting each message of the dialogue using a public key of a second private key/public key pair of the trusted body. The trusted body then uses the recorded dialogue, together with the confidential record of the relation between the identity of a user and the random identifier, to provide a means to verify the dialogue by the users. Specifically, a user cannot effectively deny that he or she sent a particular message because all messages are sent through the trusted body, and that body records all those messages.

The prior art does not disclose or suggest the use of two private/public key pairs to establish a dialogue among users, as described above.

Subramaniam, the primary reference relied on by the Examiner, discloses a method and system for providing anonymous Internet transactions. In this method, an agent monitors and maintains the anonymity of transactions between two registered users on a secure computer system. After a user registers an account, the secure system permits the user to view and to post messages on the system. Each message posted to the system passes through the agent to prevent the inadvertent disclosure of identifying information by warning the user of the disclosure and requiring the user to authorize the disclosure before posting the message. Also, in the system disclosed in Subramaniam, each party may instruct the agent to permit the disclosure of identifying information.

As the Examiner has recognized, there are a number of important differences between the present invention and the method and system disclosed in Subramaniam. In particular, Subramaniam does not disclose or suggest the use of two public/private key pairs to establish the dialogue. These two key pairs enable the trusted body to verify the identity of the user for each dialogue and also to store and to transmit the dialogue messages confidentially.

The other references of record have been reviewed, and these other references, whether considered individually or in combination, also do not disclose or suggest this feature of the invention.

Boesch, et al. describes a procedure for conducting economic transactions in a secure manner over insecure networks such as the Internet. Boesch, et al. is thus directed to security, not to verifying what was said between the parties. The Examiner cited Boesch, et al. for its discloser of generating a user identifier that is a random number. The procedure described in Boesch, et al. does not need to encrypt each received message, and clearly does not use the public key of a private/public key pair to do this.

McLaughlin discloses a procedure for processing bi-directional, anonymous or pseudo-anonymous user transactions. In this procedure, a number of digital certificates are created, and a plurality of operating modules is provided to perform various tasks. In normal operation, no one module within the system possesses enough information to determine the user's confidential identity and to connect the user to a particular transaction or to a particular anonymous or pseudo-anonymous identity.

It is noted that, in the Office Action, McLaughlin was cited for its disclosure of encrypting each message using a public key of a private/public key pair. It is important, though, the McLaughlin does not teach a user generating a separate private/public key pair and using that key pair to verify the user's identity.

Walker was cited by the Examiner for its disclosure of time stamping messages of a dialogue. This reference describes a buyer-seller protocol, in which a trusted third party may be used to determine fulfillment, adequacy and interpretation of a contract or contract offer.

Applicants ask that independent Claims 1, 13 and 17 be amended to describe the above-discussed feature of using two private/public key pairs. In particular, each of these claims is amended to indicate that each user registers with the trusted body by generating a first public/private key pair for a specific dialogue session, and sends the public key of that key pair to the trusted body. Each of Claims 1, 13 and 17 describes the further feature that the trusted body uses this public key to verify the identity of the user, and that the trusted body, among other functions, encrypts each message of the dialogue using a public key of a second public key pair of the trusted body.

In view of the above-discussed differences between Claims 1, 13 and 17 and the prior art, and because of the advantages associated with those differences, Claims 1, 13 and 17 patentably distinguish over the prior art and are allowable. Claims 2-12 and 18 are dependent from Claim 1 and are allowable therewith. Similarly, Claims 14-16 are dependent from, and are allowable with, Claim 13.

The amendments requested herein elaborate on features already described in the claims. For instance, Claims 1, 13 and 17 presently describe the feature that the users register with the trusted body, and that the trusted body verifies the identities of the user. These

claims are being amended herein to describe in more detail that registration and verification process. It is thus believed that entry of this Amendment is appropriate, and such entry is respectfully requested.

In view of the foregoing, the Examiner is respectfully requested to enter this Amendment, to reconsider and to withdraw the rejections of Claims 1-18 under 35 U.S.C. 103, and to allow these claims. If the Examiner believes that a telephone conference with Applicants' Attorneys would be advantageous to the disposition of this case, the Examiner is requested to telephone the undersigned.

Respectfully submitted,

John S. Sensny

John S. Sensny
Registration No. 28,757
Attorney for Applicant

Scully, Scott, Murphy & Presser, P.C.
400 Garden City Plaza - Suite 300
Garden City, New York 11530
(516) 7472-4343

LP:jy